AFRL-RI-RS-TR-2009-215
Final Technical Report
September 2009

THE CENTER FOR ADVANCED SYSTEMS AND ENGINEERING (CASE)

VISITING FACULTY RESEARCH PROGRAM
06-MARCH-2007 TO 05-MARCH-2009

Syracuse University

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th ABW, Wright-Patterson AFB Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2009-215 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/s/
FRANKLIN E. HOKE, Jr.
Work Unit Manager

/s/
MARGOT A. ASHCROFT, Chief
Strategic Planning and Integration Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
SEPTEMBER 2009	Final	March 2007 – March 2009

4. TITLE AND SUBTITLE

THE CENTER FOR ADVANCED SYSTEMS AND ENGINEERING (CASE)

VISITING FACULTY RESEARCH PROGRAM 06-MARCH-2007 TO 05-MARCH-2009

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
FA8750-07-2-0046

5c. PROGRAM ELEMENT NUMBER
62702F

6. AUTHOR(S)

Robert C. Hopkins, Jr.

5d. PROJECT NUMBER
558B

5e. TASK NUMBER
SY

5f. WORK UNIT NUMBER
RA

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Syracuse University
Office of Sponsored Programs
113 Bowne Hall
Syracuse, NY 13244-1200

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/RIB
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TR-2009-215

12. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA# 88ABW-2009-3818 Date Cleared: 31-August-2009

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Center for Advanced Systems and Engineering (CASE), for and on behalf of Syracuse University, has provided the services for managing the Air Force Research Laboratory Information Directorate Visiting Faculty Research Program and Summer Faculty Fellowship Program. The CASE will place highly qualified and motivated faculty members and graduate students (M.S. and Ph.D.) in science, technology, engineering and mathematics (STEM) disciplines as well as other recognized technical and newly emerges interdisciplinary areas to provide intellectually stimulating summer environment for the visitors to have enriched and rewarding experiences.

The CASE, a New York Center for Advanced Technology supported by the New York State Office of Science, Technology, and Academic Research (NYSTAR), has a long history of collaboration with the AFRL/RI. Through this endeavor, CASE supported administrative requirements for faculty members' contracts including five contract extensions and one contract spring-extension.

15. SUBJECT TERMS
Information Institute, Visiting Summer Faculty, Summer Faculty Fellowship Program, Center for Advanced Systems and Engineering.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					Franklin E. Hoke, Jr.
a. REPORT	b. ABSTRACT	c. THIS PAGE	UU	23	19b. TELEPHONE NUMBER (*Include area code*)
U	U	U			N/A

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

TABLE OF CONTENTS

1. INTRODUCTION

The Center for Advanced Systems and Engineering (CASE), for and on behalf of Syracuse University, has provided the services for managing the Air Force Research Laboratory Information Directorate Visiting Faculty Research Program and Summer Faculty Fellowship Program. The CASE will place highly qualified and motivated faculty members and graduate students (M.S. and Ph.D.) in science, technology, engineering and mathematics (STEM) disciplines as well as other recognized technical and newly emerged interdisciplinary areas to provide intellectually stimulating summer environment for the visitors to have enriched and rewarding experiences.

The CASE, a New York State Center for Advanced Technology supported by the New York State Office of Science, Technology, and Academic Research (NYSTAR), has a long history of collaboration with the AFRL/RI. Through this endeavor, CASE supported administrative requirements for faculty members' contracts including five contract extensions and one contract spring-extension.

2. FACULTY & RESEARCH AREAS

2.1 2007 Summer Professors

2.1.1 *Scott Craver, State University of New York at Binghamton*

"An Automated System for Fast Reverse-engineering of Covert Communication Algorithms, Given a Detection Oracle." We examine the problem in which an adversary is using an unknown detection algorithm, which we must reverse-engineer and then defeat. Examples of such a problem include face recognition, object tracking, watermark detection and steganalysis. We wish to understand the inner working of such a detector, including deducing its algorithm and parameters. This can be determined by its response to carefully constructed inputs, in other words an "oracle attack."
Unfortunately, not all detectors can be polled indefinitely to leak information about their inner workings. In some scenarios, we have the opportunity to submit a small set of inputs, e.g. on the order of 10-100 inputs. Thus we need fast techniques to reverse engineer an unknown detector based on few experimental interactions.

For watermarking algorithms in particular, we seek to identify specific distortions of a watermarked image that clearly identify or rule out one particular class of embedding. These experimental distortions surgical test for rapid identification of a known embedding, which we call (STRIKES) are geared towards rapid winnowing of the space of all possible embedding domains. A single test could be used, for example, to determine if a watermark is embedded in 8x8 DCT coefficients. Our goal is to assemble a collection of tests which can collectively identify an embedding method in short time. Our experiments with an unknown watermark detector gave us the opportunity to attempt some tests and gauge their selective power. These tests are presently being tested in an ongoing contest, the BOWS-II contest to break an unknown watermarking algorithm. Their ultimate effectiveness will be determined when the algorithm is finally revealed, and can be compared to the details that we deduce via reverse-engineering. In a separate track, we also examined ways to reverse-engineer parameters of additive watermarks, in particular +/- K embedding. Our techniques identify the filtering effect that occurs in an intensity histogram when data is embedded, and several improvements result in improved resolution and clarity at stronger embedding levels. The effectiveness at weak embedding levels are a matter of further investigation.

2.1.2 *Xiaohua (Edward) Li, State University of New York at Binghamton*

"Cooperative Communications for Wireless Network Capacity, Cross-Layer Design and Wireless Information Assurance." This report describes our researches in the 2007 Summer Visiting Faculty Research Program from June 2007 to August 2007. Three of our research topics within the field of wireless communication networks are included: cognitive radio network capacity, wireless information assurance for cognitive radios, and testbed development.

In the first topic, we analyze the capacity of cognitive radio-based secondary spectrum access in a broadcasting system consisting of one primary transmitter and multiple primary receivers. At the cost of a small redundancy of the SINR of primary receivers, secondary users with cognitive radios can gain a significant capacity when allowed to share the spectrum at the same time with the primary transmitter. The average transmission power and capacity of secondary users are derived, evaluated numerically, and verified by simulating a simple dynamic spectrum access protocol. The results show that the capacity depends on the distance between primary and secondary transmitters as well as the density of primary receivers.

In the second topic, we address one of the major concerns of cognitive radios when used for secondary spectrum access, i.e., the potential of interfering primary users, considering especially that cognitive radios may be misbehaved or under malicious attacks. We present a method for a cognitive radio to secure its transmission power purely from its physical-layer received signals. Built into the transceiver hardware as an independent self-check procedure, this method can guarantee the avoidance of excessive interference of cognitive radios to primary users even when the more flexible upper-layer software or policy regulator is compromised under attacks. Analysis and simulations show that the secure transmission power determined by this procedure can be very close to the ideal secondary transmission power in many practical situations, so the proposed method is helpful to guarantee both the efficiency and the security of cognitive radios.

In the third topic, a testbed is setup in order to demonstrate the cognitive radio transmissions. As a first step of the cognitive radio testbed, we have implement MC-DS-CDMA transmissions using ComBlock modules. MC-DS-CDMA is a good modulation candidate for implementing cognitive radio testbed. The major work of the testbed development is the receiver programming which addresses especially the carrier frequency offset and timing offset problem involving two distributed transmitters. This research has brought one conference papers accepted, two conference papers submitted, and two journal papers in preparation.

2.1.3 ***Vladimir V. Nikulin, State University of New York at Binghamton***

"Agile Acousto-Optic Steering for Free-Space Quantum Communication Systems."
Quantum communication is a laser communication technology that, in addition to very high data rate and low power requirements of the transmitters, offers unprecedented data security. Optical communication in general is very popular when high security is important because inherently small beam divergence angles facilitate low probability of interception and low probability of detection (LPI/LPD). However, when additional immunity to eavesdropping is required, data encryption may be necessary.
Optical communication offers the unique feature of quantum-based encryption due to the inherent properties of light used as a signal carrier. Current research efforts are aimed at using various quantum states to perform data encoding; however, polarization based techniques are still the most popular for a variety of tasks, including quantum communication (QC), quantum key distribution (QKD), and keyed communication in quantum noise (KCQ).

For many practical needs, quantum communication systems must support operation between mobile platforms. Engineering robust links; however, will depend on several innovations. In particular, successful pointing, acquisition, and tracking (PAT) require the use of a beacon signal and the capability of accurate and agile alignment of the line-of-sight (LOS) between the communicating terminals performed over a large field of regard. While mechanical devices, such as gimbals, offer relatively slow tracking over a very wide range, they lack in pointing bandwidth necessary for rejecting high frequency vibrations and beam deflection caused by the optical turbulence. In contrast, fast steering and especially non-mechanical devices, such as Bragg cells, enjoy very high bandwidth (on the order of several kHz) and could be used to compensate for high frequency distortions to the LOS caused by platform jitter and the effects of the optical turbulence.

In our previous effort a hybrid architecture that exploits the advantages of two technologies was developed to facilitate wide range connectivity by a mechanical device (Omni-Wrist gimbal) combined with high bandwidth of a narrow-range agile steerer (Bragg cell) Within the scope of the original project the emphasis was made on the synthesis of the control algorithms for the individual steerers and fusion of the technologies. It was also revealed that successful implementation of such a system requires solution of several problems associated with electro-optic phenomena pertaining to non-mechanical beam steering. These problems are addressed in this project.

2.1.4 ***Dmitry Ponomarev, State University of New York at Binghamton***

"Techniques for Improving Power/Performance Trade-offs in Cognitive Information Processing Systems." Large-scale discrete event simulations have many important applications in engineering, computer science, economics, and especially in the military. Specific examples include the models of computer and communication systems, war-gaming scenarios, simulations of battle management algorithms to optimize defense strategy and so on. These simulations, typically comprised of thousands, or even millions, of objects communicating via time-stamped messages, can easily exceed the computational and memory capacity of standalone machines. Parallel Discrete Event Simulation (PDES) systems can leverage the advantages of parallel processing to increase the performance and capacity of simulation by splitting the simulation model across a number of processing units and performing simulations in parallel.

Optimizations within the PDES systems present an extremely challenging research problem, because the sequencing constraints that dictate the order in which computations must be performed relative to each other, as well as the interactions of various simulation objects, which are in general, quite complex and highly data-dependent. Consequently, the behavior of such systems is very chaotic and the communication patterns change significantly and frequently over time. In response to a given model, the behavior of the simulator is influenced by many factors, including the configuration of several critical simulation parameters, as well as the partitioning of the simulation across the physical processors. Therefore, for most practical model, it is impossible to statically determine an optimal configuration and workload distribution across physical processing elements to provide the best possible performance for the duration of the simulation.

In this report, we present the results of our initial experiments with PDES environment demonstrating the dynamic nature of the simulations. We then describe mechanisms to monitor the simulation behavior and dynamically adjust the simulation configuration as well as workload distribution to best match the current behavior of the simulation. These ideas were developed in the course of summer research at AFRL, and the specific implementations will be designed in the future work. The basic tenet of our approach is to monitor simulation activity patterns "on-the-fly", perform the analysis of the collected statistics and dynamically reconfigure the system to provide the optimal level of performance for a given phase of execution. The specific adaptation mechanisms include dynamic workload repartitioning and object migration to control the trade-offs between workload balance and communication overhead, and object clustering to isolate the groups of simulation objects for synchronization purposes. We also plan to investigate the implications of multicore and multithreaded architectures on the performance of PDES in general and the impact on the proposed techniques in particular. It is expected that the proposed techniques will be more generally applicable to the large-scale cognitive information processing systems being developed at AFRL.

2.1.5 ***Qinru Qiu, State University of New York at Binghamton***

"Hybrid Architecture for DNA Codeword Generation, A Continuation." Cogent confabulation is a computation model that mimics the Hebbian learning, information storage, inter-relation of symbolic concepts, and the recall operations of the brain. The model has been applied to cognitive processing of language, audio and visual signals. In this project, we focus on how to accelerate the computation of confabulation based sentence completion using FPGA or multicore techniques. The results of this project may provide useful information for the architecture design of a cognitive chip which is being developed in AFRL/RITC. Three tasks have been performed. (1) Software optimization. Software for the confabulation based sentence completion has been developed in AFRL/RITC. During the summer, we optimized the software for better performance by improving the data structures and processing algorithms. More than 800X speed ups have been achieved. (2) Software analysis and profiling. Extensive software profiling has been carried out that collected information which will assist in the design of hardware architectures. (3) Architecture exploration. Architectures with different performance-cost tradeoffs have been investigated. Their performance was estimated and compared. Our analysis shows that appropriate data structures can improve the performance of the software by more than 5000X, and that the cogent confabulation algorithm is an ideal candidate for parallel processing. It also shows that although increasing the number of PEs or the size of memories can increase the performance of training and recall, the resulting cost and the performance improvements do not always exhibit a linear relation. Therefore we must choose the hardware configuration carefully in order to achieve good cost performance tradeoffs.

2.1.6 *Edmond Rusjan, State University of New York Institute of Technology*

Examination of a potential algorithm that will measure the robustness of scrambler polynomials and the application of Tsallis entropy to random number generators. Finite fields are fields with a finite number of elements. They were first studied by Evariste Galois and are also called Galois fields. They have been known initially for their mathematical beauty and applications within mathematics. More recently they have found important applications in communications engineering, where they provide the mathematical foundation of coding and scrambling. In coding, they are used as a design tool for Bose-Chaudhuri-Hocquenghem and Reed-Solomon codes. In scrambling, they provide the means to understand the properties of maximal length linear feedback shift register sequences.

This report is introduces finite fields and their properties, discusses polynomials and their factorizations, shows applications in coding and applications in scrambling and finally, discusses possibilities for future research in which the information presented in this report may be able to be used in blind decoding and descrambling.

2.1.7 *David Schwartz, Cornell University*

"SimVentive for Dummies Integration of JView and WarCon." This report proposes a generalized framework of wargame design and development that accounts for a variety of kinetic and non-kinetic effects in combat simulation. Starting with a game and simulation prototyping toolkit called SimVentive, my team and I sought to expand its capabilities to handle a multidimensional approach to wargame design. To extend current approaches, we considered a set-based model, which allows us to specify an extensible and rigorous taxonomy of game primitives. We then explain how to advance the state of wargame design, focusing on a componentized approach to visualization. The approach separates a game state from its visual representation. Thus, the views present different roles in the simulation, customization on a per-user basis, and an improved modular design of the software. The report concludes with remaining work and proposing an extension to our set model to include scoring.

2.1.8 *Qing Wu, State University of New York at Binghamton*

"Large-Scale Hybrid Computing Architecture for Neocortical Models." The first goal of the summer research work is to carry out initial investigations on deep-submicron Very Large Scale Integration (VLSI) circuit design techniques and design optimization methodologies to achieve high performance and low power for the cognitive processor that is being developed at AFRL/RITC. During my work in the summer, a workflow has been developed for logical synthesis, physical synthesis and power estimation of designs using IBM 65nm and 90nm CMOS technologies. The workflow has been tested and analyzed by the design, synthesis and simulation of a single-precision floating point (SPFP) adder and a SPFP multiplier.

In addition, we developed a large-scale hybrid neural network model on the newly installed Cell computing cluster and performed some initial test in performance and power consumption. The 128-dimensional Brain-State-in-a-Box (BSB) model has been implemented and scaled-up to run simultaneously on total of 288 IBM Cell processors. Power consumption, system reliability and networking performance were tested and analyzed. A hybrid model that combines the BSB and confabulation algorithms was also developed for intelligent character/word/sentence recognition.

2.2 2008 Summer Professors

2.2.1 *Mainak Chatterjee, University of Central Florida*

"Dynamic Spectrum Access in Cognitive Radio based Tactical Networks." With the radio spectrum becoming a scarce commodity, it is important that alternative approaches for spectrum harnessing and sharing are investigated. In this paper, we investigate how cognitive radio (CR) enabled devices can self-organize a tactical mesh network by dynamically accessing unused spectrum. The network formation is initialized by a central controller (CC) and is followed by the gradual joining of CR nodes to the mesh network in a repeated, distributed manner. The spectrum usage reports that are created by the CR nodes by constantly sensing the environment is also consulted for the resource allocation. Through extensive simulation experiments, we demonstrate how the proposed mesh creation algorithm helps minimize mesh initialization latency, reduce control signaling, reduce start-up delay, reduce collisions during network initialization, and most importantly, increase spectrum utilization.

2.2.2 *Dmitry Ponomarev, State University of New York at Binghamton*

"Object Partitioning for Parallel Discrete Event Simulation System: Implementing hmetis-based Partitioning for SPEEDES Applications." Large-scale discrete event simulations have many important applications in engineering, computer science, economics, and especially in the military. Specific examples include the models of computer and communication systems, war-gaming scenarios, simulations of battle management algorithms to optimize defense strategy and so on. These simulations, typically comprised of thousands, or even millions, of objects communicating via time-stamped messages, can easily exceed the computational and memory capacity of standalone machines. Parallel Discrete Event Simulation (PDES) systems can leverage the advantages of parallel processing to increase the performance and capacity of simulation by splitting the simulation model across a number of processing units and performing simulations in parallel.

Optimizations within the PDES systems present an extremely challenging research problem, because the sequencing constraints that dictate the order in which computations must be performed relative to each other, as well as the interactions of various simulation objects, are quite complex and highly data-dependent. Furthermore, in traditional cluster computing environments, the PDES performance and scalability are severely constrained by long communication delays when objects executing on one physical node schedule events on objects residing on the remote nodes. Fortunately, the emergence of multicore and future many-core architectures holds promise to provide breakthrough in PDES performance due to significantly reduced communication latencies across the cores residing on the same chip. However, to realize the full performance potential of PDES on muilticore architectures, a redesign of the core PDES algorithms is required.

In the course of the summer project, we performed some initial investigations of the PDES performance on multicore architectures (using the new CELL BE cluster at AFRL) to identify the new performance bottlenecks. We also identified and setup appropriate simulation tools and identified a range of interesting problems that need to be investigated in the future work.

2.2.3 *Kamesh Namuduri, University of North Texas*

"An Active Trust Model for Airborne Networks." Trust is a fundamental concept that enables cooperation and collaboration among the nodes in any network. Formal trust models are necessary for sharing information in a collaborative environment. Trust assessment methods that are commonly used in terrestrial network applications or in social networks passively gather information about other nodes and take significant amount of time for assessing trust. Such models are not suitable for tactical airborne networks which are typically deployed for short durations of time.

The summer fellowship studied an active trust model in which the nodes in a network proactively probe other nodes to assess their level of trust before sharing mission specific information. Active trust models are useful for assessing trust within short durations of time making them appropriate for airborne networks. The proposed model is based on zero-knowledge proofs.

2.2.4 *Nael Abu-Ghazaleh, State University of New York at Binghamton*

"Towards a Scalable Synthetic Cognitive Benchmark using Parallel Discrete Event Simulation." Large-scale discrete event simulations have many important applications in engineering, computer science, economics, and especially in the military. Specific examples include the models of computer and communication systems, war-gaming scenarios, simulations of battle management algorithms to optimize defense strategy and so on. These simulations, typically comprised of thousands, or even millions, of objects communicating via time-stamped messages, can easily exceed the computational and memory capacity of standalone machines. Parallel Discrete Event Simulation (PDES) systems can leverage the advantages of parallel processing to increase the performance and capacity of simulation by splitting the simulation model across a number of processing units and performing simulations in parallel. Optimizations within the PDES systems present an extremely challenging research problem, because the sequencing constraints that dictate the order in which computations must be performed relative to each other, as well as the interactions of various simulation objects, are quite complex and highly data-dependent. Furthermore, in traditional cluster computing environments, the PDES performance and scalability are severely constrained by long communication delays when objects executing on one physical node schedule events on objects residing on the remote nodes. Fortunately, the emergence of multicore and future many-core architectures holds promise to provide breakthrough in PDES performance due to significantly reduced communication latencies across the cores residing on the same chip. However, to realize the full performance potential of PDES on muilticore architectures, a redesign of the core PDES algorithms is required.

In the course of the summer project, we performed some initial investigations of the PDES performance on multicore architectures (using the new CELL BE cluster at AFRL) to identify the new performance bottlenecks. We also identified and setup appropriate simulation tools and identified a range of interesting problems that need to be investigated in the future work.

2.2.5 ***Vladimir Nikulin, State University of New York at Binghamton*** – This abstract covers the summer fellowship and extension grant. "The Optical Tracking System for Quantum Communication Terminals." Optical communications have proven to be the lowest cost and most scalable technology for keeping up with increasingly large bandwidth demands. Small light optical collimators can replace much larger radio frequency antennas and simultaneously expand the potential data rates by orders of magnitude. However, based on practical issues such as beam divergence and pointing errors, there is still a risk of interception by unauthorized parties. This risk is mitigated by appropriate use of encryption to render the received data unusable to an eavesdropper. One exciting new tool to enhance encryption strength is to exploit the quantum noise of light to add true randomization to a traditional cipher. A novel modulation format, called AlphaEta, augments the security of any desired traditional cryptographic encryption algorithm while maintaining the high data rates and long reaches desired in optical communication systems.

To create a high-speed optical communication link that uses physics-based optical encryption *and* is suitable for use on highly mobile platforms, a novel high-bandwidth tracking system was developed by our research group under AFRL funding. As part of this year's VFRP program, we worked on designing the optical trains and detection circuitry to accommodate a tracking link on a mobile platform. Synthesis of the control algorithm was conducted in an integrated fashion to address all critical points of the design. Preliminary calculation of the link budget was performed to assure that received power levels exceed the detector sensitivity. Experimental noise analysis was conducted to assure acceptable operation.

The modulation format used in the AlphaEta encrypted optical link relies on changing the phase of the optical wave and, to some degree, resembles differential phase modulation. However, dynamics of the free-space optical links makes robust operation extremely challenging due to the low power of the received signal that needs to be amplified and also due to its fluctuation caused by the pointing errors and the effects of atmospheric turbulence. These fluctuations create problems in two parts of the system. First, there is a natural phase drift present in the AlphaEta transceivers due to variations in temperature and laser wavelength. This drift is accounted for by a feedback mechanism that uses a histogram of the sampled data as a monitor and generates a correction signal applied to the phase modulator.

However, the histogram method works well only if the effects of power fluctuations are "frozen" in time, i.e. if the sampling system can collect data fast enough and feedback times are sufficiently small to assure robust control in realistic environments. Second, detection of the signal with varying power is 4 problematic, as its level can be below the sensitivity of the receiver or lead all the way to saturation. Either of the above issues must be addressed with adjustable gain control. The received signal needs to be coupled into the fiber components of the system and amplified in such a way that its power is maintained around the same level. A practical AlphaEta system uses transient control erbium doped fiber amplifiers and is able to tolerate 13 dB of power fluctuations over a time interval on the order of 1ms. This project is an experimental study that is intended to answer the question about required characteristics of a tracking system to maintain the received power within the dynamic range of the amplifiers when an encrypted signal is sent between mobile platforms over a practical atmospheric channel.

2.2.6 *Scott Craver, State University of New York at Binghamton*

"Detection of Semagram Channels." A semagram channel is a steganographic channel where no message bits! are explicitly embedded in cover data. Instead, a transmitter is required to send an unmodulated cover message chosen from a large set of allowed messages; the transmitter attempts to send a covert message through the choice of object sent. The set of allowed messages can be the same cover message subjected to different minor transformations, such as cropping or rescaling an image or resampling an audio clip prior to compression. The receiver does not have a codebook of cover messages, which makes coding and transmission nontrivial.

Semagram channels offer two interesting open problems. One is achieving a reasonable transmission capacity, or establishing bounds on this capacity. A second problem is detection of this type of covert communication; the transmission of a covert message is achieved not by embedding bits explicitly, but by choosing covers and modifications intended to be plausibly natural. I intend to study the question of whether such a steganographic paradigm could admit a reasonable data rate without being detectable to an adversary.

2.2.7 *Dijiang Huang, Arizona State University*

"Enhancing Wireless Mobile Ad Hoc Network Routing Security through Anonymous Communications." Random linear network coding based solutions allow each node in the network independently and randomly selects a set of coefficients (the construction is based on an algebraic approach) and uses them to form linear combinations of the data packets it receives. Each packet is sent along with the global encoding vector which is the set of linear transformations that the original packet goes through on its path from the source to the destination. None of previous solutions have addressed the anonymous communication capability by using network coding schemes for wireless communications. Both network coding and caching techniques require collaborations among mobile nodes. We note that the collaborations for our research are mostly localized. This requires careful protocol design for neighbors discovering and information sharing within the neighborhood. To this end, we need to investigate several research directions: (a) pseudonym-based neighbor discovering protocol to share information, such as the packet pool, however remain anonymized; (b) probability based models to monitor packets transmitted by neighbors and choose the coding scheme with high

probability that neighbors can decode it; (c) to provide end-to-end confidentiality, we can combine cryptographic methods to allow the destination to share the randomly selected coefficient selected by the source however the intermediate nodes will not change their normal network coding operations as presented in; and (d) the MANET performance of using network coding will be affected by its mobility (node density, moving speed), matrix multiplication when using linear algebraic approaches and allocated buffer for caching received packets that will introduce buffer latency.

Thus a systematical and comprehensive evaluation study must be conducted to study the tradeoffs of using network coding. This research will focus on how to design secure and anonymous communication protocols at the network layer to maximally utilize the network coding and caching techniques to increase the capacity of MANETs as well as achieve desired security and anonymity features.

2.2.8 **Qing Wu, State University of New York at Binghamton**

Research and development of large-scale BSB algorithm and confabulation algorithm for fast parallel recognition and prediction and Development and evaluation of design flow, methodology, and tools for the cognitive chip product. Modeling and simulation of human cognizance functions involve large scale mathematical models, which demand high performance computing platform. We need a novel computing architecture which meets the computational capacity and communication bandwidth of a large scale associative neural memory model.

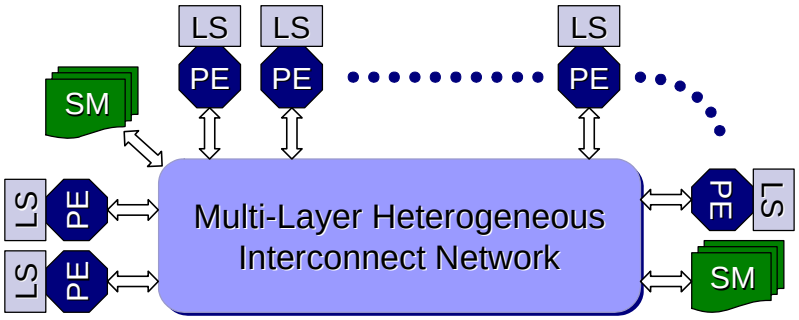

Figure 1. High performance cognitive computing system.

Figure 1 shows the targeting architecture of a high performance cognitive computing system. This system consists of multiple Processing Elements (PEs) interconnected with multi-layer heterogeneous interconnect network. All PEs have access to a local memory called Local Store (LS) and Shared Memory (SM) connected to the interconnect network.

In this report we describe the performance optimization in software and hardware solutions for a cognitive computing model called *Brain State in a Box (BSB)*. This BSB model is implemented using two different configuration of the proposed architecture. The first implementation is a software only approach using the Cell Broadband Engine. The other implementation is a hybrid configurable computing platform which uses *Field Programmable Gate Array* (FPGA) for implementing the computation.

3. CONTINUING RESEARCH PROJECTS

Additional funding was provided to allow the faculty research projects begun during the summer to continue. After the completion of the summer 2007 and 2008 projects, the following extension grants were supported.

3.1 2007 Extension Grants

3.1.1 *Qing Wu, State University of New York at Binghamton*

Cogent confabulation is a computation model that mimics the Hebbian learning, information storage, inter-relation of symbolic concepts, and the recall operations of the brain. The model has been applied to cognitive process of language, audio and visual signals. In this project, we implement the confabulation based knowledge base training function on the Cell Broadband Engine. The workload of the training function is distributed to 6 SPEs in the cell processor. One of the challenges in the implementation is the memory management. Because the local storage of the SPE is not large enough to store all the required training information, dynamic memory management techniques are developed to enable the SPE to load and write back information from/to the main memory during the training process. Preliminary software profiling has been performed to indicate the performance bottleneck and guide the software optimization. Compared to single processor training function that runs on a workstation with dual core 2GHz Pentium processor, the cell based implementation achieves 4X~9X speedups.

3.1.2 *Xiaohua (Edward) Li, State University of New York at Binghamton*

This report describes our researches in the 2007 Summer Visiting Faculty Research Program from June 2007 to August 2007. Three of our research topics within the field of wireless communication networks are included: cognitive radio network capacity, wireless information assurance for cognitive radios, and testbed development.

In the first topic, we analyze the capacity of cognitive radio-based secondary spectrum access in a broadcasting system consisting of one primary transmitter and multiple primary receivers. At the cost of a small redundancy of the SINR of primary receivers, secondary users with cognitive radios can gain a significant capacity when allowed to share the spectrum at the same time with the primary transmitter. The average transmission power and capacity of secondary users are derived, evaluated numerically, and verified by simulating a simple dynamic spectrum access protocol. The results show that the capacity depends on the distance between primary and secondary transmitters as well as the density of primary receivers.

In the second topic, we address one of the major concerns of cognitive radios when used for secondary spectrum access, i.e., the potential of interfering primary users, considering especially that cognitive radios may be misbehaved or under malicious attacks. We present a method for a cognitive radio to secure its transmission power purely from its physical-layer received signals. Built into the transceiver hardware as an independent self-check procedure, this method can guarantee the avoidance of excessive interference of cognitive radios to primary users even when the more flexible upper-layer software or policy regulator is compromised under attacks. Analysis and simulations show that the secure transmission power determined by this procedure can be very close to the ideal secondary transmission power in many practical situations, so the proposed method is helpful to guarantee both the efficiency and the security of cognitive radios.

In the third topic, a testbed is setup in order to demonstrate the cognitive radio transmissions. As a first step of the cognitive radio testbed, we have implement MC-DS-CDMA transmissions using ComBlock modules. MC-DS-CDMA is a good modulation candidate for implementing cognitive radio testbed. The major work of the testbed development is the receiver programming which addresses especially the carrier frequency offset and timing offset problem involving two distributed transmitters.

This research has brought one conference papers accepted, two conference papers submitted, and two journal papers in preparation.

3.1.3 ***Jorge Romeu, Syracuse University***

This report presents my final efforts as NOEM Project participant. It discusses work done during the four-month extension undertaken to complete my second summer research. In addition, the report describes activities to transition the DOE analyses, as I complete my work in the Project.

The Schedule charts in the Appendix show three phases separated by two weeks where I travelled to conferences abroad. The first and longest phase, comprising six weeks (76 hours) consists in research and discussions undertaken to help redefine the future course of the NOEM experimental work. Starting this Fall NOEM experimental research will transition from traditional DOE (within my applied statistics area of interests and expertise) to other modern approaches that are more computer science oriented.

The second phase, comprising four weeks (63 hours) includes a detailed statistical analysis implemented on real NOEM-generated data. Our analysis showed how it is actually possible to reduce the problem dimension via *factor screening* techniques. This phase also includes meetings among several NOEM researchers to help re-establish the new direction of the project, as already explained above.

The third and shortest phase, comprising the last four weeks (31 hours) is dedicated to phasing out and transitioning my DOE work. It includes preparation and participation in the NOEM day event, a meeting of project members where thorough and in-depth reviews of the project were given.

In almost 20 months of work, many advanced DOE procedures were overviewed. From them, several methods, appropriate for factor screening and dimension reduction of NOEM variables were identified and implemented, using our simulated data. Then, a NOEM-generated data set of 53 factors was finally obtained and, using regression selection procedures and a combination of sampling approaches, a reduction to only three factors (that describe over 96% of the problem) was successfully obtained. With this result, the theoretical study and the practical implementation of our DOE methods were demonstrated. Thence, they remain as a contribution to the NOEM project.

3.2 2008 Extension Grants

3.2.1 *Mainak Chatterjee, University of Central Florida*

"Dynamic Spectrum Access in Cognitive Radio based Tactical Networks." In this report, we investigate how cognitive radio (CR) enabled devices can self-organize to form a tactical mesh network and operate on non-dedicated (secondary) spectrum. Each node in the network constantly senses the environment and maintains an up-to-date spectrum usage report. This report is used by a central controller (CC) to initialize the network formation. Then the other CR nodes gradually join the mesh network in a repeated, distributed manner. We provide the detailed steps for the mesh creation and also propose some refinements. We also compute the spectral efficiency that is achieved through our algorithm. Through simulation experiments, we study the effectiveness of the proposed schemes on mesh initialization latency, control signaling, collision rate during network initialization, and spectrum utilization.

3.2.2 *Dmitry Ponomarev, State University of New York at Binghamton*

This report describes the infrastructure and experiences for supporting the manual object partitioning of SPEEDES applications using existing graph partitioning toolset called hMetis. This infrastructure was developed in the course of the project supported by the VFRP extension grant. We first describe the procedure used to analyze the execution traces and extract the object interaction patterns and frequencies from these traces. Then, we describe the formats of the input files accepted by hmetis and show how the SPEEDES traces were converted into the input files acceptable by hmetis. Finally, we describe how the information from hmetis output is used to manually partition the simulation object. We also show some results obtained from the execution of diems application under SPEEDES environment and illustrate that even in a simple 2-way parallel simulation, it is important to partition the objects properly to minimize communication cost. Specifically, we demonstrate that the performance difference between various partitioning of objects across simulation nodes can be as high as 15% even for 2-way simulation of relatively simple models. Finally, we describe the limitation of currently available benchmarks (i.e. diems) in terms of object partitioning and describe activities for the future work.

3.2.3 *Kamesh Namuduri, University of North Texas*

"An Active Trust Model for Airborne Networks." Airborne Networks (ANs) are three dimensional mobile ad hoc networks formed in the sky. The nodes in ANs may have communication links to ground based control stations, other ANs, as well as satellites. The nodes may move extremely fast causing dynamic topological changes to the network. ANs have stringent and very low latency requirements for entering the network as well as for transmitting data packets.

The information assurance (IA) framework for ANs, like any terrestrial network, includes authentication, authorization, access control, confidentiality, trust management, intrusion detection, and information forensics. The most critical parameter that distinguishes the IA framework for ANs from a terrestrial network is timeliness. The IA designer for ANs almost always has to balance security with the latency that comes with it.

Consider a defensive or offensive mission involving an Airborne Network that lasts for few hours. How can we build a trust model that can help achieve the desired level of information assurance for such a time-critical mission? The extension grant studied an active trust model based on the concept of zero knowledge proof, which can be used for time-critical military operations.

3.2.4 *Nael Abu-Ghazaleh, State University of New York at Binghamton*

"Towards a Scalable Synthetic Cognitive Benchmark using Parallel Discrete Event Simulation." Large-scale discrete event simulations have many important applications in engineering, computer science, economics, and especially in the military. Specific examples include the models of computer and communication systems, war-gaming scenarios, simulations of battle management algorithms to optimize defense strategy etc. These simulations, typically comprised of thousands of objects communicating via time-stamped messages, usually consume significant amounts of time if executed on standalone machines. To speed up the simulations, Parallel Discrete Event Simulation (PDES) systems execute a single simulation program on multiple processing nodes in parallel. In a PDES system, the simulation model is partitioned across multiple local simulation processes, called Logical Processes (LPs). Each LP hosts one or more simulation objects and maintains a local event queue – one for all objects executing on this LP [1]. Each LP processes events generated locally from its event queue in a time-stamped order, i.e. the earliest event first. An event scheduled on one LP can generate another event to be scheduled on a different LP – this is communicated through time-stamped event messages. Since fundamentally the simulations within various LPs proceed in parallel with each LP maintaining its own local simulation time, it is generally possible for an LP to receive an event with the earlier time stamp than its local simulation time. Since for the correct execution all events within all LPs have to be processed strictly in time-stamped order, synchronization mechanisms are needed to guarantee such correctness. PDES is a challenging application to parallelize because of its fine grained nature and complex dependency pattern.

Our work follows two complimentary goals: (1) to explore and alleviate the PDES performance bottlenecks, particularly when the simulation is executed on emerging multicore and many core hardware platforms. Multicore architectures have a potential to realize breakthrough gains in simulation scalability and performance due to the low latency of inter-core communication, but this potential can be achieved only if all subsystems of the simulation kernel are optimized. This includes such aspects as communication, workload balancing and object-partitioning across the simulation nodes. We also specifically seek to study the performance of PDES on the AFRL CELL BE cluster; (2) to develop representative benchmarks that both represent Air Force applications and expose the scale and dependency structure that justifies large scale parallel simulation.

Moreover, two secondary outcomes are desired: (1) AFRL researchers have made the case that PDES represents a reasonable metaphor for cognitive benchmarks with respect to the scale of processing and the dynamic and complex pattern of connectivity. We seek to identify or alternatively develop such models and use them to study cognitive application behavior; and (2) Given the challenging nature of parallelizing discrete event simulation, we seek to identify barriers that prevent scalability to the level of 100s of cores, and identify strategies (including hardware support) for overcoming these barriers.

4. EXPENDITURES

Under this contract expenses were billed on a faculty/week basis. The rates for the professors were established by the National Research Council for summer research fellows and are as follows.

4.1 Faculty Labor

Assistant Professor	$1,250/week
Associate Professor	$1,450/week
Full Professor	$1,650/week
Faculty Per Diem: Those faculty members whose home residence/university is more than 50 miles from AFRL/RI were entitled to:	$50/day

4.2 Other Costs Associated with Program

Occasionally expenditures for supplies were required for the program. Other expenditures made on this award included:

- (1) Roundtrip travel to and from Rome, NY / Summer Faculty Researcher

5. LIST OF ACRONYMS

CASE – Center for Advanced Systems and Engineering
STEM – Science, Technology, Engineering and Mathematics
NYSTAR – New York State Office of Science, Technology, and Academic Research
AFRL – Air Force Rome Laboratory
STRIKES – Surgical Test for Rapid Identification of a Known Embedding
LPI/LPD - Low Probability of Interception and Low Probability of Detection
QC – Quantum Communication
QKD - Quantum Key Distribution
KCQ – Keyed Communication in Quantum Noise
PAT – Pointing, Acquisition, and Tracking
LOS – Line of Sight
PDES - Parallel Discrete Event Simulation
VLSI - Very Large Scale Integration
SPFP - Single-Precision Floating Point
BSB - Brain-State-in-a-Box
CR – Cognitive Radio
CC – Central Controller
PEs – Processing Elements
LS – Local Store
SM – Shared Memory
FPGA – Field Programmable Gate Array
ANs – Airborne Networks
IA – Information Assurance
LPs – Logical Processes